A BLOCKCHAIN BASED SECURITY MODEL FOR IOT ECOSYSTEM

Sarthak Agrawal[1], Saksham Sharma[1], Surjeet Balhara[1]

[1]Department of Electronics and Communication Engineering, Bharati Vidyapeeth College of Engineering, New Delhi, India.

ABSTRACT

The use of IoT devices has been increasing exponentially with time and this raises serious concerns for the overall protection of the huge IoT Network's and the database's associated with it. While there are many proposed approaches to deal with different security related aspects in IoT, one of the potential solutions to such issues is Blockchain. Blockchain is a rapidly emerging technology and is used in various fields. Blockchain technology has features like decentralisation and immutability which guarantees security. A blockchain based security model has been proposed in this paper for securing IoT devices from various security threats. Finally, proposed approach and its implementation using blockchain to secure IoT Ecosystem is discussed to make IoT ecosystem more secure.

KEYWORDS: Authentication, Blockchain, Data Protection, IoT, Security.

1. INTRODUCTION:

Nowadays, the uses of Internet of Things(IoT) can be seen everywhere ranging from applications in education or medical purposes to military operations and logistics. One of the major concerns with the IoT devices is security of system as well the data associated with it. IoT is all about data, But with the growth IoT technology in recent years, One can easily see the growth in cyber-crime cases including Denial-of-Service attack, Key Logging attack and many more[1]. Although many techniques and technologies are proposed earlier to solve the security related problems of IoT, but none of them proved to be legitimate in order to secure the IoT devices completely. IoT devices can be hacked very easily making them a soft target for the hackers [2]. When we consider appliances like mobile phones, smart TV's and automatic cars, lack of security can be a major concern. Devices with low security can be a easy target for the hackers. A very systematic and effective approach of Securing IoT devices from malicious attackers has been our top-most priority and some aspects of which can also been in work proposed by kshetri[3]. Currently, a centralized model of networking is used by IoT device's[4].

While there are many solutions for data security in IoT devices, one of the most effective solutions is blockchain. Most of the people know Blockchain as a technology used for Cryptocurrency (bitcoin, ethereum etc) trading [5]. But it is not limited to only Cryptocurrency. It can also be used for data security and a variety of purposes. Blockchain can handle a huge number of devices [6]. The main problem in most of the techniques used for data security is that they largely focus on security of the central device or hub which act as a mediator through which communication between two or more devices is possible. In Blockchain technology, a central hub is no longer needed for mediating communication between different devices. Every device in a network interacts with every other device in order to share a particular information or data. Blockchain helps to store data in a distributed manner to several locations rather than storing it in one place[7].

i. Insufficient privacy protection – Privacy is one of the major concern for modern era and due to lack of effective tools, it becomes our top most priority to resolve it as soon as possible in order to have a secure environment to work in and blockchain is most suited technology for this purpose.

ii. Software and firmware vulnerabilities – Nowadays, Hackers are looking for various types of vulnerabilities in software's and underlying firmware in order to gain access to its user data that can be a major trouble for any IoT Device. Blockchain is nearly impossible to hack as it requires 51% of the total computing power of network which makes it so much reliable and effective.

Lack of data security is a major concern for the IoT devices. IoT devices can be easily hacked and hackers can steal crucial data and may use that for malicious purpose's[8]. Such devices having low security are a soft target for the hackers. So, it is very important that devices must have strong security to keep data safe.

Internet of Things, in the modern era, is a distributed network of intelligent objects with software and data management being provided by centralized third party entities. Not only does this client-server model add to the limitations of the network, it also forces users to place their trust on third-party entities to manage their data and not misuse it. Therefore, the research problem to be solved is leveraging blockchains and peer-to-peer data storage techniques for IoT data privacy, where each user has complete authority over their data without trusting any third-party entities to manage IoT software or data.

Some of the major security problems in IoT devices are listed below:

i. Lack of encryption.

ii. Application vulnerabilities.

iii. Lack of trusted execution environment.

iv. Vendor security posture.

v. Insufficient privacy protection.

vi. Software and firmware vulnerabilities.

In this paper a security model by integrating Blockchain (BC) in IoT ecosystems is proposed. This model will help in achieving high security and privacy. Therefore, IoT ecosystem can be secured by using blockchain based decentralized and distributed model. In this paper, importance of Blockchain for securing IoT, it's scope and different advantages are discussed.

Once the smart contracts are deployed on the blockchain network such as Ethereum Mainnet or any other network. The Entire code for smart contract and front end has been written on VS Code platform.

In first section of this paper, Introduction to world of IoT devices and ways to secure them using blockchain technology are discussed. In the second section, the related work done by different researchers has been discussed ,then in third section model on securing IoT devices through blockchain smart contracts is proposed. Lastly, In the fourth and fifth section we have discussed the results followed by conclusion of the research done.

2. RELATED WORK:

Rapid demand in adoption of blockchain technology, many researchers have proposed different approaches for the new technology. Kshetri et al[9] had given insights on the use of security services for current applications, to highlight the state of the art techniques that are currently used to provide these services, to describe their challenges.

In the sector of healthcare using blockchain which is well mention in the work proposed by Fakhri et al[10]. In the paper by Singh et al[11], a new way for data authentication and authorization was proposed that not only increases the credibility but also suggest new ways of protecting and securing data through blockchain.

IoT System and Applications - In previous work by Rathee et.al.[12], relationship, investigates challenges in blockchain IoT applications, and surveys the most relevant work in order to analyse how blockchain could potentially improve the IoT. Alghamdi et.al. [13] analyse the security risks of digital wallets in Android, which is the most popular mobile operating system. Not only cryptocurrency wallets but IoT and Blockchain finds its application in voting system with is brilliantly explained By Kouzinopoulos et.al. [14] in their paper.

The above studies mainly focus on data security, data authentication and privacy. A proof-of-authenticity model proposed by Rehman et.al. [15] is also another security concept implemented through smart contract. Our model's advantage in comparison with other works lies in its simplicity and ease of use. Our research addresses the different issues related to security and data privacy.

In research done by Jeon et.al.[16], they have conferred the applications and the different threats of IoT. They also have proposed the future solutions to deal with the different IoT threats. They discussed some issue related to blockchain as data privacy, scalability, availability and various types of consensus algorithms.

In the paper proposed by Dorri Jesus et.al.[17], they have discussed several IoT Scenarios where blockchain can be effective.

Author Huang et al. [18], proposed a method consisting of three modules to deal with the security issues and protect one's privacy in the smart home. The first module consists of a data collecter that collects users' data from the smart home and then sends that data to data receiver module which has the function to store data in two different sets. The final result module make sure that the user's access to data is controlled to protect the privacy of the user. This will ensures that only the real user can have the access of data. Same type of methodology is proposed by Cho et al.[19] .

The use of blockchain for various IoT domains such as the Internet of energy proposed by Liang et al.[20], Internet of finance proposed by Minoli et al.[21], the Internet of healthcare things proposed by Mohanta et al.[22], smart vehicles based on IoT proposed by Kim et al. [23]. Following the trend of leveraging blockchain for IoT, a number of schemes for secure sharing of data over blockchains have been explored by the researcher community such as Novo et.al.[24]. In research done by Yu et.al.[25], they proposed CALYPSO for sharing of private data in which data is stored on-chain and authorities that are formed over the blockchain are solely responsible for enforcing access control policies. However, this design is not suitable for real world scenarios consisting of large number of IoT devices connected to each other and a huge amount of data is transferred every second.

Similarly, Jesus et al., [26] proposed a system where transactions are handled by the Blockchain between different parties before granting permissions, however how such transactions are not addressed, and only owners have the right to commit any changes in the policies. The design allows different updates or distributions of decryption keys to be done in a very autonomously manner on the blockchain back-end side without any owner's interventions.

3. PROPOSED WORK:

In our model we propose a ethereum based crypto wallet for secure and efficient data transfer. The model consist of a dashboard containing two fields: First is the hashed address where the required amount of coins are to sent and the second field is the required amount of data to be sent. The most common use of blockchain is in transactions of cryptocurrencies. However, its use in not limited to only cryptocurrencies. Financial institutions and banks are using blockchain to increase the speed of transaction and also reduce the cost of operation.

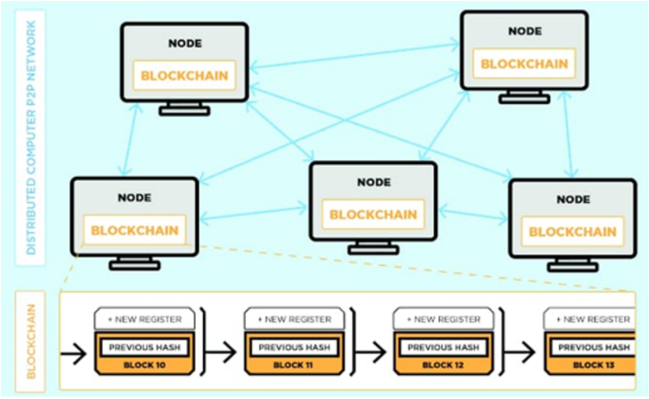


Figure 1: Architecture of Blockchain Nodes[27].

Figure 1 shows the architecture and interconnectivity of various nodes used in blockchain for mining purposes.

We used a very well-known hashing algorithm known as SHA-3 designed by Guido Bertoni, Joan Daemen, Michaël Peeters and Gilles Van Assche[28]. Keccack, their cryptographic algorithm for encryption won the NIST award in 2009 and thereafter was regarded as a default SHA encryption scheme. It was released by NIST on August 5, 2015.

Keccak is significantly faster than SHA-2 (from 25% to 80%, depending on implementation). It uses the sponge construction[29]. Analogous to a sponge, the data is first absorbed and then the filtered result is squeezed out. While absorbing, message blocks are XORed into a subset of the state. Then it's transformed as one element. During the ongoing process of obtaining the result, the output blocks are altered with necessary state transformations.

SHA-3 was designed in a way that it eliminates all the drawbacks that were present in SHA-2 and make it more reliable and trustworthy. A Transition from SHA-2 to SHA-3 requires a critical look into the application architecture and should be considered wisely after all the successful tests[30].

The proposed cryptocurrency wallet contains a collection of key pairs, each pair consists of a private key and a public key. The private key can be regarded as a randomly generated stream of numbers. From the private key, we will use a one-way cryptographic function to generate a public key (K). From the public key (K), a one-way cryptographic hash function is used to generate a transaction address.

We have build an Ethereum based Cryptocurrency wallet web app which uses mainly two technologies: Ethereum based Smart Contracts and React. blockchain technology is mainly implemented via Smart Contracts and that is exactly what we have done. In this Research Paper, We build our front-end using a very well known and reliable front end library called React.

React generally divides the whole web page into a number of components such that the rendering of the web page becomes easy and very less time is required to reload the entire web page if certain changes are done. The part of web page where the change is to be done or any bug is to be removed is first identified via the component in which it is situated and then the need-full changes are being made. Secondly, we used Solidity language of writing Our Smart Contracts.

The below Flowchart shows the flow that is being followed when the user tries to login in our cryptocurrency wallet.

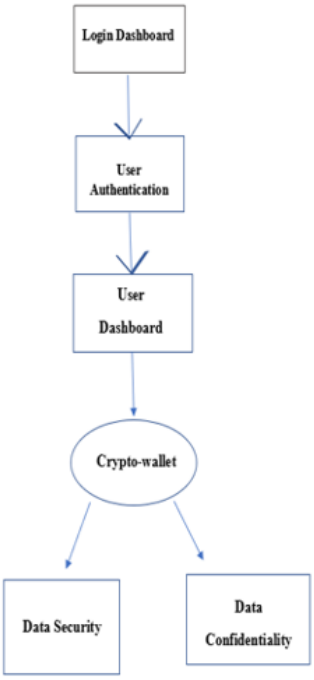
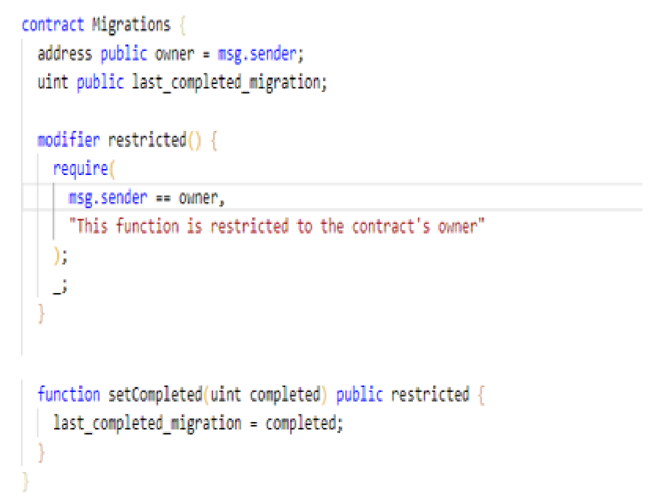


Figure 2: Flowchart representing the process from user login to data security.

In the flowchart shown in figure 2, flow of user login to data security by the wallet is shown. After the successful authentication of user, the user is directed to his/her dashboard where they integrate their metamask wallet with the crypto dashboard and after a successful login the user can send the required amount to the given hashed address. Thus, the receiver address becomes encrypted and the overall confidentiality and Integrity of data is maintained.

4. RESULT:

It can be seen that the overall security of IoT Devices is greatly enhanced by employing the latest blockchain technology. Also, the Process overhead and Network traffic overhead was exponentially reduced thereby increasing the overall efficiency and maximizing the data security to make transaction system more trustable and reliable . Our proposed model include a hash function to generate the secret hash address to secure the transactional data. Further the hash address can only be decrypted using the private key only available with the receiver. Our proposed model guarantees data security and provides an interface for bilateral transfer of transactional data . Figure 3 and 4 shows the screenshots of code written for smart contract in VS Code:

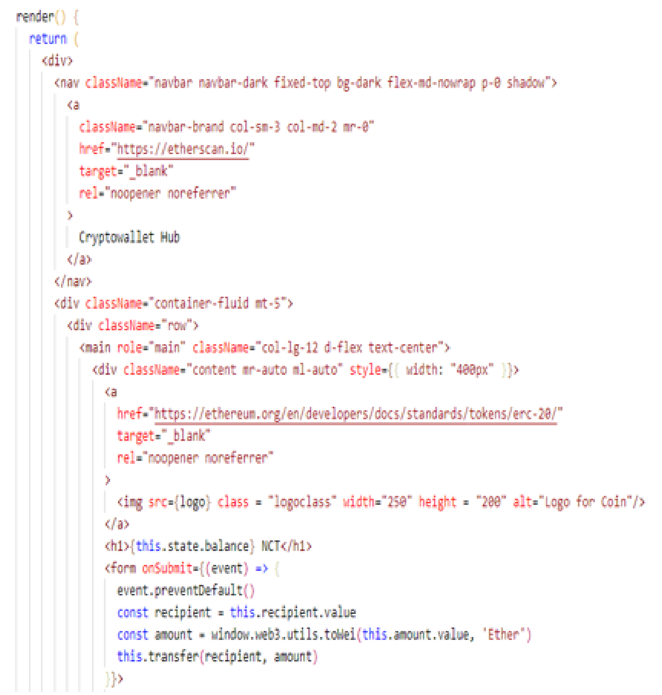


```
contract Migrations {
  address public owner = msg.sender;
  uint public last_completed_migration;

  modifier restricted() {
    require(
      msg.sender == owner,
      "This function is restricted to the contract's owner"
    );
    _;
  }

  function setCompleted(uint completed) public restricted {
    last_completed_migration = completed;
  }
}
```

Figure 3: Screenshot of Smart contract written in Solidity using VSCODE as a platform.



```
render() {
  return (
    <div>
      <nav className="navbar navbar-dark fixed-top bg-dark flex-md-nowrap p-0 shadow">
        <a
          className="navbar-brand col-sm-3 col-md-2 mr-0"
          href="https://etherscan.io/"
          target="_blank"
          rel="noopener noreferrer"
        >
          Cryptowallet Hub
        </a>
      </nav>
      <div className="container-fluid mt-5">
        <div className="row">
          <main role="main" className="col-lg-12 d-flex text-center">
            <div className="content mr-auto ml-auto" style={{ width: "400px" }}>
              <a
                href="https://ethereum.org/en/developers/docs/standards/tokens/erc-20/"
                target="_blank"
                rel="noopener noreferrer"
              >
                <img src={logo} class = "logoclass" width="250" height = "200" alt="Logo for Coin"/>
              </a>
              <h1>{this.state.balance} NCT</h1>
              <form onSubmit={(event) => {
                event.preventDefault()
                const recipient = this.recipient.value
                const amount = window.web3.utils.toWei(this.amount.value, 'Ether')
                this.transfer(recipient, amount)
              }}>
```

Figure 4: Another Screenshot of code snippet from the project.

REFERENCES:

I. Huh, S., Cho, S. and Kim, S., 2017, February. Managing IoT devices using blockchain platform. In 2017 19th international conference on advanced communication technology (ICACT) (pp. 464-467). IEEE.

II. Agrawal, R., Verma, P., Sonanis, R., Goel, U., De, A., Kondaveeti, S.A. and Shekhar, S., 2018, April. Continuous security in IoT using blockchain. In 2018 IEEE international conference on acoustics, speech and signal processing (ICASSP) (pp. 6423-6427). IEEE.

III. Košťál, K., Helebrandt, P., Belluš, M., Ries, M. and Kotuliak, I., 2019. Management and monitoring of IoT devices using blockchain. Sensors, 19(4), p.856.

IV. Taylor, P.J., Dargahi, T., Dehghantanha, A., Parizi, R.M. and Choo, K.K.R., 2020. A systematic literature review of blockchain cyber security. Digital Communications and Networks, 6(2), pp.147-15s6.

V. Dhar, S. and Bose, I., 2021. Securing IoT devices using zero trust and blockchain. Journal of Organizational Computing and Electronic Commerce, 31(1), pp.18-34.

VI. Mohanta, B.K., Jena, D., Ramasubbareddy, S., Daneshmand, M. and Gandomi, A.H., 2020. Addressing security and privacy issues of IoT using blockchain technology. IEEE Internet of Things Journal, 8(2), pp.881-888.

VII. Srivastava, G., Parizi, R.M., Dehghantanha, A. and Choo, K.K.R., 2019, November. Data sharing and privacy for patient iot devices using blockchain. In International Conference on Smart City and Informatization (pp. 334-348). Springer, Singapore.

VIII. Guin, U., Cui, P. and Skjellum, A., 2018, July. Ensuring proof-of-authenticity of IoT edge devices using blockchain technology. In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 1042-1049). IEEE.

IX. Kshetri, N., 2017. Can blockchain strengthen the internet of things?. IT professional, 19(4), pp.68-72.

X. Fakhri, D. and Mutijarsa, K., 2018, October. Secure IoT communication using blockchain technology. In 2018 International Symposium on Electronics and Smart Devices (ISESD) (pp. 1-6). IEEE.

XI. Singh, M., Singh, A. and Kim, S., 2018, February. Blockchain: A game changer for securing IoT data. In 2018 IEEE 4th World Forum on Internet of Things (WF-IoT) (pp. 51-55). IEEE.

XII. Rathee, G., Sharma, A., Kumar, R. and Iqbal, R., 2019. A secure communicating things network framework for industrial IoT using blockchain technology. Ad Hoc Networks, 94, p.101933.

XIII. Alghamdi, T.A., Ali, I., Javaid, N. and Shafiq, M., 2019. Secure service provisioning scheme for lightweight IoT devices with a fair payment system and an incentive mechanism based on blockchain. IEEE Access, 8, pp.1048-1061.

XIV. Kouzinopoulos, C.S., Spathoulas, G., Giannoutakis, K.M., Votis, K., Pandey, P., Tzovaras, D., Katsikas, S.K., Collen, A. and Nijdam, N.A., 2018, February. Using blockchains to strengthen the security of internet of things. In International ISCIS Security Workshop (pp. 90-100). Springer, Cham.

XV. Rehman, M., Javaid, N., Awais, M., Imran, M. and Naseer, N., 2019, December. Cloud based secure service providing for IoTs using blockchain. In 2019 IEEE Global Communications Conference (GLOBECOM) (pp. 1-7). IEEE.

XVI. Jeon, J.H., Kim, K.H. and Kim, J.H., 2018, January. Block chain based data security enhanced IoT server platform. In 2018 International Conference on Information Networking (ICOIN) (pp. 941-944). IEEE.

XVII. Dorri, A., Kanhere, S.S. and Jurdak, R., 2017, April. Towards an optimized blockchain for IoT. In 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI) (pp. 173-178). IEEE.

XVIII. Huang, J., Kong, L., Chen, G., Wu, M.Y., Liu, X. and Zeng, P., 2019. Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism. IEEE Transactions on Industrial Informatics, 15(6), pp.3680-3689.

XIX. Cho, S. and Lee, S., 2019, January. Survey on the Application of BlockChain to IoT. In 2019 International Conference on Electronics, Information, and Communication (ICEIC) (pp. 1-2). IEEE.

XX. Liang, X., Zhao, J., Shetty, S. and Li, D., 2017, October. Towards data assurance and resilience in IoT using blockchain. In MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM) (pp. 261-266). IEEE.

XXI. Minoli, D. and Occhiogrosso, B., 2018. Blockchain mechanisms for IoT security. Internet of Things, 1, pp.1-13.

XXII. Mohanta, B.K., Satapathy, U., Panda, S.S. and Jena, D., 2019, December. A novel approach to solve security and privacy issues for iot applications using blockchain. In 2019 International Conference on Information Technology (ICIT) (pp. 394-399). IEEE.

XXIII. Kim, S.K., Kim, U.M. and Huh, J.H., 2019. A study on improvement of blockchain application to overcome vulnerability of IoT multiplatform security. Energies, 12(3), p.402.

XXIV. Novo, O., 2018. Scalable access management in IoT using blockchain: A performance evaluation. IEEE Internet of Things Journal, 6(3), pp.4694-4701.

XXV. Yu, Y., Li, Y., Tian, J. and Liu, J., 2018. Blockchain-based solutions to security and privacy issues in the internet of things. IEEE Wireless Communications, 25(6), pp.12-18.

XXVI. Jesus, E.F., Chicarino, V.R., De Albuquerque, C.V. and Rocha, A.A.D.A., 2018. A survey of how to use blockchain to secure internet of things and the stalker attack. Security and Communication Networks, 2018.

XXVII. https://www.stefanjunestrand.com/blog/what-is-blockchain/

XXVIII. Bertoni, G., Daemen, J., Peeters, M. and Assche, G.V., 2011, August. Duplexing the sponge: single-pass authenticated encryption and other applications. In International Workshop on Selected Areas in Cryptography (pp. 320-337). Springer, Berlin, Heidelberg.

XXIX. Bertoni, G., Daemen, J., Peeters, M. and Assche, G.V., 2013, May. Keccak. In Annual international conference on the theory and applications of cryptographic techniques (pp. 313-314). Springer, Berlin, Heidelberg.

XXX. Dworkin, M.J., 2015. SHA-3 standard: Permutation-based hash and extendable-output funct.